

AMENDMENTS TO THE CLAIMS

1 - 15. (Cancelled)

16. (New) A method of supporting a roaming service in a wireless network having an authentication server and a plurality of access points (APs) connected to the authentication server, the method comprising:

deriving from a known master key a first-level security key to be shared between a station STA and an AP with which the STA attempts to associate when the STA attempts to associate with one of the plurality of APs ;

deriving from the first-level security key a second-level security key to be shared between the STA and at least one neighbor AP, the at least one neighbor AP neighboring to the AP with which the STA attempts to associate; and

providing the second-level security key to the at least one neighbor AP,

wherein when the STA attempts to roam to the at least one neighbor AP, the at least one neighbor AP pre-authenticates the STA with the second-level security key.

17. (New) The method of claim 16, wherein the first-level security key is a first-level pairwise master key and the second-level security key is a second-level pairwise master key.

18. (New) The method of claim 17, further comprising deriving from the first-level pairwise master key in the AP with which the STA attempts to associate a pairwise transient key.

19. (New) The method of claim 17, further comprising deriving from the second-level pairwise master key in the at least one neighbor AP a pairwise transient key.

20. (New) The method of claim 17, wherein deriving a second-level security key to be shared between the STA and at least one neighbor AP from the first-level security key comprises deriving from the first-level pairwise master key the second-level pairwise master key, considering a Medium Access Control (MAC) address of the STA.

21. (New) The method of claim 16, wherein the at least one neighbor AP is an AP to which the STA can roam without passing through a coverage area of another AP.

22. (New) The method of claim 21, wherein the STA attempts to associate with the AP by roaming from the at least one neighbor AP.

23. (New) In a wireless network having an authentication server and a plurality of access points (APs) connected to the authentication server, a method of supporting a roaming service in one of the plurality of APs, comprising:

receiving from the authentication server a first-level security key derived from a known master key when a station (STA) attempts to associate with an AP;

deriving from the first-level security key a second-level security key for at least one neighbor AP, the at least one neighbor AP neighboring to the AP with which the STA attempts to associate; and

providing to the at least one neighbor AP the second-level security key,

wherein when the STA attempts to roam to the at least one neighbor AP, the at least one neighbor AP pre-authenticates the STA with the second-level security key.

24. (New) The method of claim 23, wherein the first-level security key is a first-level pairwise master key and the second-level security key is a second-level pairwise master key

25. (New) The method of claim 24, further comprising deriving from the first-level pairwise master key a pairwise transient key.

26. (New) The method of claim 24, further comprising deriving from the second-level pairwise master key in the at least one neighbor AP a pairwise transient key.

27. (New) The method of claim 24, wherein deriving a second-level security key for at least one neighbor AP from the first-level security key comprises deriving from the first-level pairwise master key the second-level pairwise master key, considering a Medium Access Control (MAC) address of the STA.

28. (New) The method of claim 23, wherein the at least one neighbor AP is an AP to which the STA can roam without passing through a coverage area of another AP.

29. (New) The method of claim 28, wherein the STA attempts to associate with the AP by roaming from the at least one neighbor AP.

30. (New) A method of generating a security key in a wireless network having an authentication server and a plurality of access points (APs) connected to the authentication server, the method comprising:

receiving from the authentication server a first-level pairwise master key derived from a known master key;

deriving from the first-level pairwise master key a pairwise transient key; and

deriving from the first-level pairwise master key a second-level pairwise master key for at least one neighbor AP.

31. (New) The method of claim 30, further comprising deriving from the second-level pairwise master key in the at least one neighbor AP a pairwise transient key.

32. (New) The method of claim 31, wherein deriving a second-level pairwise master key for at least one neighbor AP from the first-level pairwise master key comprises deriving from the first-level pairwise master key the second-level pairwise master key, considering a Medium Access Control (MAC) address of a station (STA).

33. (New) In a wireless network having an authentication server and a plurality of access points (APs) connected to the authentication server, a method of generating a security key in a target AP to which a station (STA) associated with a serving AP attempts to roam, the method comprising:

receiving from the serving AP a second-level pairwise master key;

deriving from the second-level pairwise master key a pairwise transient key; and

deriving from the second-level pairwise master key a new second-level master key for at

least one neighbor AP.

34. (New) The method of claim 33, further comprising deriving a new second-level master key for at least one neighbor AP from the second-level pairwise master key comprises deriving from the second-level pairwise master key the new second-level pairwise master key, considering a Medium Access Control (MAC) address of the STA.

35. (New) A method of supporting a roaming service for a station (STA) in a wireless network having a server for authenticating the STA and managing accounting for the STA and a plurality of access points (APs) connected to the authentication server, the method comprising:

receiving from a first AP association information regarding association in the server of the STA with the first AP;

notifying by the server at least one neighbor AP that the STA has completely associated with the first AP, the at least one neighbor AP neighboring to the first AP and when the STA attempts to roam to the at least one neighbor AP;

sending to the at least one neighbor AP a security key generated based on the association information when the at least one neighbor AP requests the security key for the STA,

wherein the at least one neighbor AP authenticates the STA using the security key received from the server.

36. (New) The method of claim 35, wherein the association information includes a first-level pairwise master key and a Medium Access Control (MAC) address of the STA.

37. (New) The method of claim 36, wherein the first-level pairwise master key is derived from a master key by the first AP.

38. (New) The method of claim 36, wherein the security key that the server sends to the at least one neighbor AP is a second-level pairwise master key derived from the first-level pairwise master key.

39. (New) A method of supporting a roaming service for a station (STA) in a wireless network having a server for authenticating the STA and managing accounting for the STA and a plurality of access points (APs) connected to the authentication server, the method comprising:

deriving a first-level pairwise master key to be shared between the STA and a first AP by the server when the STA attempts to associate with the first AP being one of the plurality of APs; deriving from the first-level pairwise master key a second-level pairwise master key; and providing to at least one neighbor AP neighboring to the first AP the second-level pairwise key,

wherein when the STA attempts to roam to the at least one neighbor AP, the at least one neighbor AP authenticates the STA with the second-level pairwise master key.

40. (New) The method of claim 39, wherein the first AP sends a Medium Access Control (MAC) address of the STA to the server, for generation of the first-level pairwise master key.

41. (New) The method of claim 40, wherein deriving a first-level pairwise master key further comprises deriving from a master key known to the server by the server the first-level pairwise master key.

42. (New) The method of claim 39, wherein deriving a second-level pairwise master key from the first-level pairwise master key comprises deriving from the first-level pairwise master key the second-level pairwise master key, considering a MAC address of the at least one neighbor AP by the server.